ABSTRACT

The present invention provides a flexible, tamper-resistant authentication system, or personal authentication device (PAD), which can support applications in authentication, authorization and accounting. The PAD stores at least one public key associated with a certificate authority (CA) and receives one or more digital certificates, which may be authenticated based on the stored CA public keys. The PAD outputs a service key that, depending on the application, may be used to gain access to a controlled space, obtain permission for taking a certain action, or receive some service. The operation of the PAD and the nature of the service key may be determined by digital certificates that it receives during operation. Using a stored PAD private key that is kept secret, the PAD may perform a variety of security-related tasks, including authenticating itself to a user, signing service keys that it generates, and decrypting content on received digital certificates.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com